Région académique
AUVERGNE-RHÔNE-ALPES

Technologie, Sciences de l'Ingénieur et Techniques Industrielles

Wireshark

https://www.wireshark.org/

Gratuit

OS : Windows / Mac OS

Niveau : Lycée

Point(s) positif(s) :	Point(s) négatif(s) :
- Open-source - Portable	- En anglais

Présentation :

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Source Wikipedia

Utilisation :

Un exemple d'utilisation de Wireshark est la lecture et l'analyse de trame issu du protocole TCP/IP. Pour lire ("sniffer") les information échanger entre le pc et un autre hôte du réseau il faut :

- Lancer la lecture de trames (menu *Capture / Start)*
- Appliquer le filtre permettant de ne voire que les trames souhaitées :

IP.addr == adresse IP de l'autre hôte (valider avec *Apply*)

Les trames échangées apparaissent alors dans la fenêtre du logiciel, elles sont découpées en octets, eux même convertis en hexadécimal. Un affichage graphique permet aussi de repérer les différentes couches du protocole.